UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,682	09/27/2001	Jin Kun Lin	1409/3	4982

25297 7590 12/21/2004

JENKINS & WILSON, PA
3100 TOWER BLVD
SUITE 1400
DURHAM, NC 27707

EXAMINER	
MEUCCI, MICHAEL D	
ART UNIT	**PAPER NUMBER**
2142	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/966,682	LIN, JIN KUN	
	Examiner	Art Unit	
	Michael D Meucci	2142	

-- The MAILING DATE of this communication app ars on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 September 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09/27/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 1 objected to because of the following informalities: It is believed by the examiner that the applicant meant to specify --a secure web page-- on lines 5-6 of the claim in place of "a non-secure web page". Correction is required if appropriate.

2. Claim 15 objected to because of the following informalities: It is believed by the examiner that the applicant meant to specify --non-secure control applets-- on line 4 of the claim in place of "secure control applets". Correction is required if appropriate.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-23 rejected under 35 U.S.C. 103(a) as being unpatentable over Roberts et al. (U.S. 6,295,551 B1) hereinafter referred to as Roberts, in view of Curtis (U.S. 5,870,544).

a. As per claim 1, Roberts teaches: a control applet associated with a web browser on a client computer for sending and receiving form and pointer update information received from a user co-browsing a webpage (abstract and line 52 of column 3 through line 49 of column 4); at least one callback function for detecting a form modification or a pointer update from a user of the web browser and for sending a

form modification or pointer update message to the control applet in response to determining that the form modification or pointer update occurs in the web page (lines 4-49 of column 4); and a co-browse server for receiving form modification and pointer update messages from the control applets and for broadcasting the messages to participants in a co- browsing conference (abstract, lines 17-49 of column 7, and item 20 of Fig. 1).

Although Roberts teaches the callback function for detecting a form modification or pointer update from a user of the web browser, Roberts fails to teach the function determining whether the form modification or pointer update occurs in a secure or non-secure web page. However, Curtis discloses "a means for establishing a secure connection between a Java Applet and a secure web server for protocols other than HTTPS" (lines 47-49 of column 3), thereby detecting the security of the web pages.

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have a function that determines whether the form modification or pointer update occurs in a secure or non-secure web page. "It would therefore be a distinct advantage to have a method and apparatus for using the web browser's installed certificates to set up and establish an encrypted session between a Java Applet and a secure web server for protocols other than HTTPS. It would be further advantageous if the method and apparatus would only require the use of a secure web server and no additional services (i.e., additional servers)" (lines 35-44 of column 3 of Curtis). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to have a function that determines

whether the form modification or pointer update occurs in a secure or non-secure web page in the system as taught by Roberts.

b. As per claim 2, Roberts teaches: the applet is downloaded using the hyper-text transfer protocol (abstract, line 56 of column 10 through line 4 of column 11, and lines 1-24 of column 20).

Roberts fails to teach: the applet is downloaded using the secure hyper-text transfer protocol (HTTPS). However, Curtis discloses: "The present invention defines a method, an apparatus and a computer program product for establishing a secure connection between a Java Applet and a secure web server for protocols other than HTTPS via the use of a Java Security Service. More specifically, the present invention uses the web browser's installed certificates to setup and establish an encrypted session between the Java Applet and the secure web server," (abstract).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have the applet downloaded using the secure hyper-text transfer protocol (HTTPS). "The secure connection is then used to retrieve the certificates required by the Java security service (Abstract of Curtis). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to have the applet downloaded using the secure hyper-text transfer protocol (HTTPS) in the system as taught by Roberts.

c. As per claim 3, Roberts teaches: the non-secure control applet is downloaded using the non-secure hyper-text transfer protocol (HTTP), (abstract, line 56 of column 10 through line 4 of column 11, and lines 1-24 of column 20).

d. As per claims 4-6, Roberts teaches: [with respect to claim 4] the callback function includes a first callback function for detecting form modifications (lines 32-49 of column 4 and lines 24-52 of column 16); and a second callback function for detecting pointer updates (lines 58-65 of column 3 and lines 1-17 of column 8). Roberts also teaches: [with respect to claims 5-6] the co-browse server is adapted to broadcast a form modification or pointer update message to control applets of participants in a co-browsing conference in response to receiving the form modification or pointer update from the control applet (lines 10-23 of column 4).

Although Roberts teaches utilizing a second applet containing greater functionality (lines 55-64 of column 4), which thereby would be notifying the appropriate applet, Roberts fails to teach: notifying the appropriate secure or non-secure control applet [with respect to claim 4]. However, Curtis teaches HTTP (lines 19-32 of column 2), secure connections, SSL and HTTPS (lines 11-25 of column 3). The addition of HTTPS applets disclosed in Curtis, utilized as the "applet representative of that (greater) functionality" in Roberts, would allow the notification of the appropriate secure or non-secure control applet.

Roberts also fails to teach: broadcasting to secure/non-secure control applets in response to receiving updates from the respective secure/non-secure control applets [with respect to claims 5-6]. Since it has been shown that secure/non-secure applets can be notified of a modification, it is obvious that the co-browser would broadcast the notification to applets of their respective type (secure/non-secure) on the co-browsing participants' computer(s).

It would have been obvious to utilize HTTP and HTTPS applets and to broadcast to the appropriate (secure/non-secure) applets in response to receiving the form modification or pointer update from the respective secure/non-secure control applets in the system of Roberts. "If later on during the visual communication the user computer requires greater functionality, the server will then download a second user applet containing the necessary functionality. In this way, the server decreases the resource collection of the user computer in both time and space while enabling the functions of the resource that the user wishes to enable," (lines 58-64 of column 4 in Roberts). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to notify the appropriate secure or non-secure control applets and to broadcast to the appropriate (secure/non-secure) applets in response to receiving the form modification or pointer update from the respective secure/non-secure control applets in the system as taught by Roberts.

e. As per claim 7, Roberts teaches: the control applets are adapted to display form modifications and pointer updates to conference participants in response to the messages received from the co-browse server (lines 4-23 of column 4).

f. As per claims 8 and 16, Roberts teaches: establishing a web conference that allows multiple participants to simultaneously view web documents (abstract); detecting form modifications and pointer updates by the participants in web documents (line 52 of column 3 through line 49 of column 4); in response to determining that a form modification or pointer update occurs, notifying a co-browse server via an applet (lines 4-23 of column 4).

Roberts fails to teach: determining whether the form modifications and pointer updates occur in secure or non-secure web documents; and notifying co-browser via the appropriate (secure/non-secure) applet. However, Curtis teaches HTTP (lines 19-32 of column 2), secure connections, SSL and HTTPS (lines 11-25 of column 3). The addition of HTTPS applets disclosed in Curtis, utilized as the "applet representative of that (greater) functionality" in Roberts, would allow the notification of the appropriate secure or non-secure applet. Once the appropriate applet is notified, the co-browser is notified as per Roberts (lines 4-23 of column 4). It is for these reasons that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to determine whether the form modifications and pointer updates occur in secure or non-secure web documents and to notify the co-browser via the appropriate respective (secure/non-secure) applet in the system as taught by Roberts.

g. As per claims 9 and 17, Roberts teaches: downloading, to each of the participants, a shared web page (lines 58-65 of column 3 and lines 5-13 of column 10); including form update and pointer synchronization scripts for detecting form updates and pointer actions by the participants and for notifying the co- browse server (abstract, line 65 of column 4 through line 18 of column 5, and line 45 of column 13 through line 47 of column 14).

h. As per claims 10 and 18, Roberts teaches: establishing a web conference including downloading the non-secure control applets to each of the participants (abstract, line 56 of column 10 through line 4 of column 11, and lines 1-24 of column 20).

Roberts fails to teach: downloading the secure control applets to each of the participants. However, because Curtis has already established utilization of secure applets (lines 11-25 of column 3), it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to download the secure control applets to each of the participants in the same manner as the non-secure control applets. Motivation therein lies in the combination of downloading the secure control applets taught by Curtis to each of the participants for the same reasoning that Roberts downloads the non-secure control applets, as a communication means (abstract of Roberts). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to download the secure control applets to each of the participants in the system as taught by Roberts.

i. As per claims 11 and 19, Roberts teaches: detecting form modifications and pointer updates includes executing the form update and pointer synchronization scripts (line 39 of column 12 through line 2 of column 13).

j. As per claims 12 and 20, Roberts fails to teach: notifying a co-browse server via a secure control applet includes notifying the co-browse server via encrypted messages. However, Curtis discloses: "It would therefore be a distinct advantage to have a method and apparatus for using the web browser's installed certificates to set up and establish an encrypted session between a Java Applet and a secure web server for protocols other than HTTPS," (lines 35-39 of column 3).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to notify a co-browse server via encrypted messages. It would be

further advantageous if the method and apparatus would only require the use of a secure web server and no additional services (i.e., additional servers)," (lines 39-42 of column 3 in Curtis). It is for this reason that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to notify a co-browse server via encrypted messages in the system as taught by Roberts.

k. As per claims 13 and 21, Roberts teaches: notifying a co-browse server via a secure control applet includes notifying a co-browse server via an HTTP JAVA control applet (line 63 of column 17 through line 15 of column 18).

l. As per claims 14-15 and 22-23, Roberts teaches: at the co-browse server, in response to receiving a form modification or pointer update in a web page, broadcasting the form modification or point update to the conference participants' control applets (lines 4-23 of column 4).

Roberts fails to teach: in response to receiving a form modification or pointer update in a secure/non-secure web page, broadcasting the form modification or point update to the conference participants' respective secure/non-secure control applets. However, Curtis teaches HTTP (lines 19-32 of column 2), secure connections, SSL and HTTPS (lines 11-25 of column 3). The addition of HTTPS applets disclosed in Curtis, as described above, allow differentiation between secure and non-secure applets.

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have the co-browse server, in response to receiving a form modification or pointer update in a secure/non-secure web page, broadcast the form

modification or point update to the conference participants' respective secure/non-secure control applets.

Once the appropriate applet is notified of the type (secure/non-secure) of web page, the co-browser is notified as per Roberts (lines 4-23 of column 4). It is for these reasons that one of ordinary skill in the art at the time of the applicant's invention would have been motivated to at the co-browse server, in response to receiving a form modification or pointer update in a secure/non-secure web page, broadcast the form modification or point update to the conference participants' respective secure/non-secure control applets in the system as taught by Roberts.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ingrassia, Jr. et al. (U.S. 5,951,652) discloses dependable data element synchronization mechanism.

Koneru et al. (U.S. 5,966,705) discloses tracking a user across both secure and non-secure areas on the internet, wherein the users is initially tracking using a globally unique identifier.

Pommier et al. (U.S. 6,047,314) discloses remote collaboration system with multiple host computers using multiple applications.

Podgorny et al. (U.S. 6,078,948) discloses platform-independent collaboration backbone and framework for forming virtual communities having virtual rooms with collaborative sessions.

Subramaniam et al. (U.S. 6,081,900) discloses secure internet access.

England (U.S. 6,144,991) discloses system and method for managing interactions between users in a browser-based telecommunications network.

Sallette (U.S. 6,155,840) discloses system and method for distributed learning.

Gutfreund et al. (U.S. 6,192,394 B1) discloses inter-program synchronous communications using a collaboration software system.

Brown (U.S. 6,195,691 B1) discloses method and apparatus for creating and using dynamic universal resource locations.

Pacifici et al. (U.S. 6,230,171 B1) discloses markup system for shared HTML documents.

Wellner et al. (U.S. 6,628,767 B1) discloses active talker display for web-based control of conference calls.

Ohkado et al. (U.S. 6,668,276 B1) discloses HTML file acquisition method, information terminal support device, and storage medium for storing a software product for acquiring HTML files.

Aravamudan et al. (U.S. 6,732,145 B1) discloses collaborative browsing of the internet.

Ohkado et al. (U.S. 2001/0016873 A1) discloses method for acquiring content information, and software product, collaboration system and collaboration server for acquiring content information.

Lee et al. (U.S. 2002/0035603 A1) discloses method for collaborative-browsing using transformation of URL.

Esenther (U.S. 2002/0138624 A1) discloses collaborative web browsing.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Meucci at (571) 272-3892. The examiner can normally be reached on Monday-Friday from 9:00 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jack Harvey, can be reached at (571) 272-3896. The fax phone number for this Group is (703) 872-9306.

Communications via Internet e-mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [michael.meucci@uspto.gov].

All Internet e-mail communications will be made of record in the application file. PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MDM

JASON CARDONE
PRIMARY EX
AU:2145